Toward Better Depth Lower Bounds: Strong Composition of XOR and a Random Function

Nikolai Chukhin, Alexander S Kulikov, Ivan Mihajlin

March 6, 2025

Motivation

We want to prove:

$$P \neq NC^1$$

.

Motivation

We want to prove:

$$P \neq NC^1$$

.

$n^{3.1}$ circuit lower bound for an explicit f.

Motivation

We want to prove:

$$P \neq NC^1$$

.

$n^{3.1}$ circuit lower bound for an explicit f.

$n^{2.1}$ circuit lower bound for an explicit f without random restrictions.

Motivation

We want to prove:

$$P \neq NC^1$$

.

$n^{3.1}$ circuit lower bound for an explicit f.

$n^{2.1}$ circuit lower bound for an explicit f without random restrictions.

$n^{2.1}$ almost circuit lower bound for an explicit f without random restrictions.

Karchmer-Wigderson games

Definition

The Karchmer-Wigderson game for $f : \{0,1\}^n \to \{0,1\}$:

- Alice gets $x \in \{0,1\}^n$ such that $f(x) = 0$.
- Bob gets $y \in \{0,1\}^n$ such that $f(y) = 1$.
- Their goal is to find $i \in [n]$ such that $x_i \neq y_i$.

The Karchmer-Wigderson relation for f:

$$\mathrm{KW}_f = \{(x, y, i) \mid x, y \in \{0,1\}^n, i \in [n], f(x) = 0, f(y) = 1, x_i \neq y_i\}.$$

KRW conjecture

Definition

For $f : \{0,1\}^m \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$, *the block-composition* $f \diamond g : (\{0,1\}^n)^m \to \{0,1\}$ is defined by

$$(f \diamond g)(x_1, \dots, x_m) = f(g(x_1), \dots, g(x_m)),$$

where $x_1, \dots, x_m \in \{0,1\}^n$.

Conjecture (The KRW conjecture)

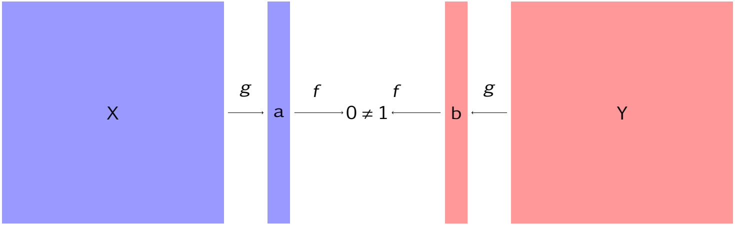
Let $f, g : \{0,1\}^m \to \{0,1\}$ *be non-constant functions. Then*

$$\mathrm{CC}(\mathrm{KW}_{f \diamond g}) \approx \mathrm{CC}(\mathrm{KW}_f) + \mathrm{CC}(\mathrm{KW}_g).$$

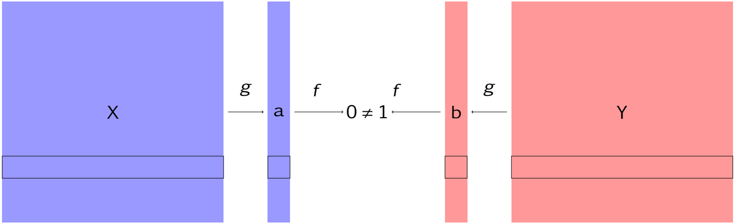
Theorem

KRW conjecture implies $\mathsf{P} \not\subseteq \mathsf{NC}^1$.

Composition of KW games



Composition of KW games



Solve KW_f on (a, b) first, then solve KW_g on (X_i, Y_i).

Strong Composition

Definition

$\mathrm{KW}_f \circledast \mathrm{KW}_g$ for $f : \{0,1\}^n \to \{0,1\}$:

- Alice gets $X \in \{0,1\}^{n \times m}$ such that $(f \circ g)(X) = 0$.
- Bob gets $Y \in \{0,1\}^{n \times m}$ such that $(f \circ g)(Y) = 1$
- Their goal is to find $i, j \in [n]$ such that $X_{i,j} \neq Y_{i,k}$ and $g(X_i) \neq g(Y_i)$.

Universal relation

The universal relation of length n,

$$\mathrm{U}_n = \{(x, y, i) \mid x, y \in \{0, 1\}^n, i \in [n], x_i \neq y_i\}.$$

Known results

- [Edmonds, Impagliazzo, Rudich, Sgall, 01] and [Håstad, Wigderson, 98] :

$$\mathrm{CC}(\mathrm{U}_n \diamond \mathrm{U}_n) = 2n - o(n).$$

- [Gavinsky, Meir, Weinstein, Wigderson, 16], improved by [Meir, Koroth, 19] (proof by measure argument):

$$\mathrm{CC}(f \diamond \mathrm{U}_n) = \log \mathrm{L}(f) + n - O(\log^* n).$$

- [Mihajlin, Smal 21], improved by [Wu 23]:

$$\exists g: \ \mathrm{CC}(\mathrm{U}_n \diamond g) \geq 2n - o(n).$$

Meir 23 :

$$\forall f, \exists g \mathrm{CC}(\mathrm{KW}_f \circledast \mathrm{KW}_g) \geq \mathrm{CC}(\mathrm{KW}_f) - 0.96m + n - O(\log(mn))$$

Results

Theorem

With probability $1 - o(1)$*, for a random function* $f\colon \{0,1\}^{\log m} \to \{0,1\}$*, any protocol solving* $\mathrm{KW}_{\mathrm{XOR}_m} \circledast \mathrm{KW}_f$ *has at least* $n^{3-o(1)}$ *leaves, where* $n = m \log m$*.*

Results

Theorem

With probability $1 - o(1)$*, for a random function* $f\colon \{0,1\}^{\log m} \to \{0,1\}$*, any protocol solving* $\mathrm{KW}_{\mathrm{XOR}_m} \circledast \mathrm{KW}_f$ *has at least* $n^{3-o(1)}$ *leaves, where* $n = m \log m$*.*

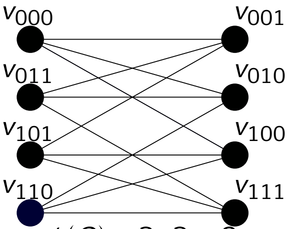
Theorem

For any 0.49*-balanced function* $f\colon \{0,1\}^{\log m} \to \{0,1\}$*, any protocol solving* $\mathrm{KW}_{\mathrm{XOR}_m} \circledast \mathrm{KW}_f$ *has at least* $n^{2-o(1)} \cdot \mathrm{L}_{\frac{3}{4}}(f)$ *leaves, where* $n = m \log m$*.*

Khrapchenko's Graph for XOR_3

For a biparite graph $G(A \sqcup B, E)$, let

$$\psi(G) = \mathrm{avgdeg}(G, A) \cdot \mathrm{avgdeg}(G, B).$$



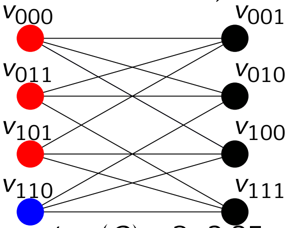
$\psi(G) = 3 \cdot 3 = 9$

Khrapchenko's Graph for XOR_3

For a biparite graph $G(A \sqcup B, E)$, let

$$\psi(G) = \mathrm{avgdeg}(G, A) \cdot \mathrm{avgdeg}(G, B).$$

Blue ones sent 0, Red ones sent 1.



$\psi_{\mathrm{red}}(G) = 3 \cdot 2.25 = 6.75$

$\psi_{\mathrm{blue}}(G) = 3 \cdot 0.75 = 2.25$

Lower bound for XOR

Theorem

Any protocol that solves $\mathrm{KW}_{\mathrm{XOR}_m}$ *has depth at least* $2 \log m$.

Proof.

Lower bound for XOR

Theorem

Any protocol that solves $\mathrm{KW}_{\mathrm{XOR}_m}$ *has depth at least* $2\log m$*.*

Proof.

- $\psi(G_r) = n^2$, G_r is the graph at the root

Lower bound for XOR

Theorem

Any protocol that solves $\mathrm{KW}_{\mathrm{XOR}_m}$ *has depth at least* $2 \log m$*.*

Proof.

- $\psi(G_r) = n^2$, G_r is the graph at the root
- $\psi(G_l) \leq 1$, , G_r is a graph at the leaf.

Lower bound for XOR

Theorem

Any protocol that solves $\mathrm{KW}_{\mathrm{XOR}_m}$ *has depth at least* $2 \log m$*.*

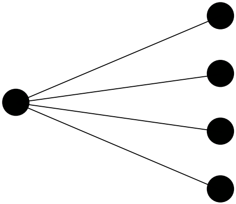
Proof.

- $\psi(G_r) = n^2$, G_r is the graph at the root
- $\psi(G_l) \leq 1$, , G_r is a graph at the leaf.
- ψ is subadditive.

□

$\mathrm{OR}_d \circledast f$

Hard on rectangle $A \times B$ if f is hard to approximate and both A and B have large projections on every row.



Plan

- First stage: Go down the protocol trying to maximize $\psi(G)$ until the average degree of one part becomes less $\tilde{O}(1)$.

Plan

- First stage: Go down the protocol trying to maximize $\psi(G)$ until the average degree of one part becomes less $\tilde{O}(1)$.
- Second stage: Focus on a node of degree $d = \tilde{\Omega}(\psi(G))$ and its neighbors. This is almost the same as solving $\mathrm{OR}_d \circledast f$, which requires $d \cdot \mathrm{L}_{\frac{3}{4}}(f)$.

Open problems

- Replace $L_{\frac{3}{4}}(f)$ by L.

Open problems

- Replace $L_{\frac{3}{4}}(f)$ by L.
- Replace strong composition by the regular one.

Open problems

- Replace $L_{\frac{3}{4}}(f)$ by L.
- Replace strong composition by the regular one.
- Prove $P \neq NC_1$

Thank You!